Remarks and Arguments

Claims 1-37 have been presented for examination. Claims 12-16 and 21-27 have been withdrawn.

Claims 1, 4-5, 7-9, 11, 17-18, 20, 34 and 36-37 have been rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,564,320 (de Silva) in view of U.S. Patent No. 6,772,331 (Hind.) The examiner comments that de Silva discloses the invention as claimed with the exception that it does not disclose that the generated certificate includes an identifier for the first node. However, the examiner asserts that Hind shows such an identifier and concludes that it would have been obvious to combine de Silva and Hind in order to allow the system to more securely monitor the generated certificates.

The present invention concerns a method and system for generating a certificate that includes information identifying a first intermediate node that both receives a certificate request from a client and forwards the request to a second node. In particular, the request includes an identifier that identifies the node that made the request. The second node actually generates the certificate including the first node identifier. The identifier in the certificate can later be used to more quickly revoke the certificate should the first node become untrustworthy.

The de Silva reference discloses a certificate generation system in which a local server (202, Figure 6) generates a certificate request form and receives a request for a certificate from a client (102). The local server (202) forwards this request to a central server (104) that acts as a certificate authority and actually generates the certificate. This arrangement allows the local server to customize the certificate request form and, when a request is received, to convert the request to a standardized form that is then sent to the certificate authority. In this manner, the certificate authority always receives the same standardized request and, therefore, the formatting work that must be performed by the certificate authority is reduced. Thus, the local server (202) acts as a node that both receives a certificate request and forwards that request to a second node that actually generates the certificate. However, as the examiner admits, the de Silva patent does not disclose either that the request to the certificate authority include an

identifier that identifies the local server (202) or that the certificate generated by the certificate authority includes any information identifying the local server (202).

The Hind reference discloses an arrangement for pairing two wireless devices. This pairing arrangement uses a certificate authority to bind the public key of a mobile wireless device to an identifier for that device. In this arrangement, an administrative server makes a request to a mobile device for a device identifier that uniquely identifies the device. The device returns the device identifier to the administrative server. Then, either the device or the administrative server generates a public/private key pair and this key pair is sent, together with the device identifier to the certificate authority. The certificate authority issues a certificate binding the key pair to the mobile device identifier. In the Hind system there is no request from a client to generate a certificate. To the extent that Hind has anything equivalent to the first node recited in the claims, the administrative server would correspond to the first node because it makes the request to the certificate authority for the certificate. However, the certificate that is generated does not include an identifier that would identify the administrative server. Instead, it includes an identifier for the mobile device. Therefore, if the administrative server becomes untrustworthy, the identifier in the certificate cannot be used to quickly revoke certificates generate by it.

The examiner proposes to combine de Silva and Hind to arrive at a combination that obviates the present invention. However, the proposed combination does not render the claimed invention obvious. First, de Silva does not identify any nodes in the certificate and Hind identifies a mobile device, not the node that makes the certificate request to the certificate authority. A combination of de Silva and Hind would produce a distributed system which could be used to tie mobile devices together by using the local server of de Silva as the administrative server of Hind. However, this combination does not generate a certificate including an identifier that identifies the local server. Since neither de Silva nor Hind is directed to the problem solved by applicant's invention – identifying a node that makes a request for a certificate so that the certificate can be more easily revoked, the combination could not suggest substituting an identifier for the local server or the administrative server for the mobile device identifier actually disclosed in Hind.

The present claims particularly point out this difference. For example, claim 1 recites, in lines 3-10, "at a first node ... receiving a request to issue a certificate ... forwarding said request to a second node, wherein said request includes a first identifier that identifies the first node ... and generating a certificate that includes said first identifier (emphasis added)." As discussed above, neither de Silva nor Hind discloses that the server which makes the certificate request to the certificate authority makes a certificate request which includes an identifier identifying the node that made the request. Nor can the combination of these references suggest this recited combination also as discussed above. Thus, claim 1 patentably distinguishes over the cited combination of references.

Claims 4, 5, 7, 9 and 11 are dependent, either directly or indirectly, on claim 1 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 1. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 7 recites that the certificate includes a time stamp associated with the request. The examiner points to de Silva as disclosing such a time stamp. However, de Silva only discloses that the certificate authority verifies that a certificate issued by it is not expired. Although no timestamp is explicitly mentioned, certainly any implied timestamp would be associated with the certificate and its issuance rather than with the request. Nonetheless, the examiner claims that it would have been obvious to include a timestamp in the certificate that refers to the request. However, the examiner does not point to any reference that shows such a time stamp or suggests such a timestamp. Thus, this rejection fails to establish *prima facie* obviousness. See MPEP §2143.03.

Claim 17 distinguishes over the cited combination in the same manner as claim 1. For example, claim 17 recites, in lines 6-10, "receiving a request from a registration authority to issue a certificate on behalf of a principal; and in response to receipt of said request, generating said certificate that includes at least a registration authority identifier associated with said registration authority." As discussed above, neither de Silva nor Hind discloses that a generated certificate include an identifier associated with a server that might correspond to the recited "registration authority", such as de Silva server 202 or, possibly, the Hind administrative server. Nor can the combination of these

references suggest this recited combination also as discussed above. Thus, claim 17 patentably distinguishes over the cited combination of references.

Claims 18 and 20 are dependent on claim 17 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 17. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 20 recites that the certificate includes a time stamp associated with the request in a manner similar to claim 7. Therefore, claim 20 distinguishes over the cited combination of references in the same manner as claim 7.

Claim 34 contains limitations that parallel those in claims 1 and 17 and distinguishes over the cited combination of references in the same manner as claims 1 and 17. Claims 36 and 37 are dependent on claim 34 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 34. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 37 recites a means that provides an indication that a certificate is untrustworthy based on a comparison of a node identifier in the certificate with the node identifier of an untrustworthy node on a certificate revocation list. The examiner points to de Silva as disclosing revocation of certificates. However, de Silva does not disclose how the certificates are revoked as recited in claim 37. Consequently, de Silva does not disclose the limitations in claim 37 and claim 37 patentably distinguishes over de Silva and Hind.

Claims 2-3, 6, 10, 19 and 35 have been rejected under 35 U.S.C. §103(a) over de Silva in view of Hind and further in view of U.S. Patent No. 6,308,277 (Vaeth.) The examiner comments that de Silva and Hind teach all of the claimed limitations except that they do not explicitly disclose that the certificate request contains an identifier that identifies the principal. However, the examiner asserts that the Vaeth reference discloses a request with such an identifier and concludes that it would have been obvious to combine Vaeth with de Silva and Hind in order to allow more secure monitoring of transactions.

Claims 2, 3, 6 and 10 are dependent on claim 1 and incorporate the limitations thereof. These claims distinguish over the combination of de Silva and Hind as discussed above. Adding Vaeth to the combination does not supply the limitations that are missing in the combination of de Silva and Hind. In particular, Vaeth discloses a certification system that includes a registration authority and a certificate authority. However, rather than the registration authority receiving a request for a certificate from a client and then sending that request to the certificate authority, in the Vaeth system, the request for the certificate is sent directly to the certificate authority from the client. The certificate authority then contacts the registration authority to authenticate the client. In this manner the registration authority does not have to pass the request through from the client to the certificate authority and also pass the certificate from the certificate authority to the client. Vaeth does not disclose or suggest that the server which makes the certificate request to the certificate authority makes a certificate request which includes an identifier identifying the node that made the request as recited in claim 1. Consequently, claims 2, 3, 6, and 10 distinguish over the cited combination in the same manner as claim 1.

In the same manner, claim 19 is dependent on claim 17 and claim 35 is dependent on claim 34. As discussed above, claims 17 and 34 distinguish over the cited de Silva and Hind combination. Since adding the Vaeth reference to this latter combination does not change the combination such that it would render claims 17 or 34 obvious, claims 19 and 35 also distinguish over the cited combination.

Claims 28-33 have been rejected under 35 U.S.C. §103(a) over de Silva in view of Vaeth. The examiner comments that de Silva and teaches all of the claimed limitations except that it does not explicitly disclose a principal identifier, a principal key and a registration identifier associated with a registration authority. However, the examiner asserts that Vaeth discloses these elements.

Vaeth is discussed above. It does not disclose the registration identifier. Claim 28, for example, recites "program code ... for generating by a certification authority a certificate ... includes ... a registration identifier associated with said registration authority." Thus, claim 28 patentably distinguishes over the cited combination of de Silva and Vaeth. Claim 29 depends on claim 28 and, therefore, incorporates the

limitations of claim 28 and patentably distinguishes over the cited combination in the same manner as claim 28. Claim 30 contains limitations that parallel those in claim 28 and distinguishes in the same manner. Claims 31-33 depend on and incorporate the limitations of claim 30 and thus distinguish over the cited combination in the same manner as claim 30.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, he is invited to call applicants' attorney at the number listed below. The examiner is hereby authorized to charge any fees or direct any payment under 37 C.F.R. 1.17, 1.16 to Deposit Account number 02-3038.

Respectfully submitted

Paul E. Kudirka Date: 2/11/05

Paul E. Kudirka, Esq. Reg. No. 26,931
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656